eCH-0219 IAM Glossar

Name	IAM Glossar
eCH-Nummer	eCH-0219
Kategorie	Standard; Best Practice; Hilfsmittel; White Paper; Addendum
Reifegrad	Definiert; Experimentell; Implementiert; Verbreitet; Auslaufend
Version	1.0
Status	**In Arbeit;** Entwurf; Vorschlag; Genehmigt; Abgelöst; Aufgehoben, Sistiert
Beschluss am	JJJJ-MM-TT
Ausgabedatum	JJJJ-MM-TT
Ersetzt Version	- <Minor Change; Major Change>
Voraussetzungen	<Vorausgesetzter Standard>
Beilagen	<Beilage>
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	<Fachgruppe> <Autoren>
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

<Kurze Zusammenfassung des Zwecks des Dokuments>

Inhaltsverzeichnis

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument

bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

1 Einleitung

Der vorliegende Standard definiert die wichtigsten Begriffe für IAM-Lösungen im föderalen E-Government Schweiz und bildet damit die Grundlage aller eCH Standards im Bereich IAM.

Die aufgenommenen Begriffe umfassen Stakeholder, Prozesse, Services bis zu Implementationsdetails in föderierten und nicht föderierten IAM-Lösungen. Begriffe aus aktuellen internationalen Standards werden zu den definierten Begriffen in Beziehung gesetzt und damit verständlicher gemacht.

1.1 Status

<Zutreffendes fett markieren>

In Arbeit: **Der Gebrauch ist nur innerhalb der Fachgruppe, bzw. im Expertenausschuss zugelassen.**

Entwurf: Das Dokument wurde von den zuständigen Referenten aus dem Expertenausschuss zur öffentlichen Konsultation freigegeben und entsprechend publiziert.

Vorschlag: Das Dokument wird dem Expertenausschuss zur Genehmigung TT-MM-JJJJ vorgelegt, ist aber normativ noch nicht gültig.

Genehmigt: Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

Abgelöst: Das Dokument wurde durch eine neue, aktuellere Version ersetzt. Die Benutzung ist zwar noch möglich, es wird aber empfohlen, die neuere Version einzusetzen.

Aufgehoben: Das Dokument wurde von eCH zurückgezogen. Er darf nicht mehr genutzt werden.

1.2 Anwendungsgebiet

2 Begriffe

2.1 Authentifikator

Der Authentifikator ist das funktionale Abbild des Authentifizierungsmittels der Realwelt. Mit der Funktion eines Authentifikators wird in der Regel aus einem Eingabewert (Challenge) und einem geheimen Wert ein Ausgabewert erzeugt. Je nach Ausprägung muss der geheime Wert durch einen zweiten Faktor (PIN) aktiviert werden

Synonyme: Authentifizierungsfunktion, engl. Authentificator

2.2 Attribut / Attribute

Semantisches Abbild einer einem Subjekt zugeordneten Eigenschaft, die das Subjekt näher

beschreibt. Der Identifikator und die Credentials sind ebenfalls Attribute.

Ein Attribut setzt sich zusammen aus den Meta-Attributen Attributname (z.B. „Schuhgrösse“), Attributtyp (z.B. „Integer“) und Attributwert (z.B. „39“).

Im Stellvertretungsfall besitzt die E-Identity des Stellvertreters für eine gewisse Zeit eine Menge von Attribute der E-Identity des vertretenen Subjekts.

Persönliche Attribute: Attribute die einer natürlichen Person gehören. Dieser alleine muss über die Weitergabe von diesen Attributen entscheiden können.

Enterprise Attribute: Attribute die einer Organisation gehören. Diese entscheidet im Rahmen geltender Gesetze und Verträge über die Weitergabe der Attribute. Der einzelne Benutzer innerhalb der Organisation spielt im Rahmen dieser Entscheidung eine sekundäre Rolle.

2.3 Attribute Assertion Service

Eine Entität, die Attributbestätigungen über eine definierte Schnittstelle ausstellt.

2.4 Attribute Service

Der Attribute Service pflegt zeitaktuell ein oder mehrere Attribute für definierte Subjekte.

2.5 Attribut-Autorität (AA)

Eine Attribut-Autorität ist ein Register oder sonstiges Verzeichnis mit einem Attribute Service zur Pflege von Attributen und einem Attribute Assertion Service zur Ausstellung von Attribute Assertions.

eCH-0167: Informationslieferant, der über eine definierte Schnittstelle (STIAM-Sender) Attribute für die STIAM-Community bereitstellt.

Synonyme: Attribute Authority, Datenlieferant, Informationslieferant

2.6 Attribute-Based Access Control (ABAC)

Konzept dynamischer Zuteilung von Zugriffsrechten basierend auf Attributen des Subjekts.

2.7 Attributaggregation

Der Begriff der Attributaggregation wird von N. Klingenstein in „Attribute Aggregation and Federated Identity“ [ref] genau beschrieben. Man versteht darunter den Prozess, Attribute zu einer bekannten digitalen Identität von verschiedenen Quellen abzufragen und zusammenzustellen.

2.8 Attributbestätigung

Bestätigung eines Attributs durch eine Attribute Authority. Entspricht einer SAML 2.0 Attribute Assertion [SAML 2.0 TechOverview].

Synonym: Attribute Assertion

2.9 Auditing

a) Überprüfung der Policy-Konformität

b) Aufzeichnung aller Aktionen und Entscheide zur Gewährleistung der Nachvollziehbarkeit

2.10 Authentifizierung

Authentifizierung ist der Vorgang der Überprüfung einer behaupteten E-Identity eines Subjekts nach bestimmten Vorgaben. Das angestrebte Sicherheitsniveau der Authentifizierung bestimmt diese Vorgaben.

Spezialfall eIDAS: dynamische Authentifizierung (kein SSO)

Synonyme: Authentifikation, Authentisierung (todo! Fussnote bemerkung)

2.11 Authentifizierungs-Anfrage

Eine Authentifizierungs-Anfrage wird vom Subjekt an den Authentication Service gesendet. Dieser initialisiert die Überprüfung der behaupteten E-Identity.

Synonym: Authentication Request

2.12 Authentifikation-Autorität (AuthnA)

Eine AuthnA stellt einen Authentication Service zur Verfügung, gegen den sich das Subjekt authentifizieren kann. Der Authentication Service benutzt Credentials, die von einem Credential Service ausgestellt werden. Der Credential Service kann ein Bestandteil der AuthnA sein. Beispiele für Authentifikation-Autoritäten sind IdPs (nach SAML), OpenID Provider und MobiID Provider.

Synonym: Authentication Authority

2.13 Authentication Proxy

Ist AuthnA(1) nicht in der Lage, einen Nutzer zu authentifizieren, kann er unter bestimmten Umständen als Authentication Proxy agieren, indem er selber einen eigenen Authentication Request an einen weiteren AuthnA sendet. Die Antwort vom AuthnA(2) kann der AuthnA(1) dann dazu verwenden, eine eigene Response zu generieren. Die Authentication Proxy Funktion wird im SAMLv2 Standard beschrieben und weitgehend definiert, heisst dort Identification Proxy.

2.14 Authentication Service

Der Authentication Service überprüft mittels der Authentifizierungsmittel, ob der Zugreifende (Subjekt) der ist, der er behauptet zu sein.

2.15 Authentifizierungsbestätigung

Die Authentifizierungsbestätigung ist der Nachweis, welcher der Identity Provider nach einer erfolgreichen Authentifizierung des Subjektes ausgestellt wird. Die Authentifizierungsbestätigung ist für einen bestimmten Zeitraum gültig und hat eine der in diesem Dokument beschriebenen Vertrauensstufen.

Beispiele:

Bei Security Assertion Markup Language (SAML) [1] ist die Authentifizierungsbestätigung die „Authentication Assertion“ und wird vom (SAML) Identity Provider ausgestellt.

Bei OIDC [2] ist die Authentifizierungsbestätigung das sogenannte „ID Token“ und wird vom „Authorization Server“ ausgestellt.

Bei Kerberos ist die Authentifizierungsbestätigung ein „Ticket Granting Ticket“ (TGT) und wird vom Kerberos Distribution Center (KDC) ausgestellt.

2.16 Authentifizierungsfaktor

Authentifizierungsfaktoren sind Informationen und/oder Prozesse, die zur Authentifizierung eines Subjektes verwendet werden können. Authentifizierungsfaktoren können auf vier verschiedenen Merkmalen oder auch Kombinationen davon beruhen:

- besitzabhängiger Authentifizierungsfaktor: beruht auf Besitz (etwas, das das Subjekt besitzt, z.B. Zertifikat, Hardware-Token mit privatem Schlüssel, elektronischer Pass oder ID-Karte),

- kenntnisabhängiger Authentifizierungsfaktor: beruht auf Wissen (etwas, das das Subjekt weiss, z.B. Passwort, PIN),

- inhärenter Authentifizierungsfaktor: beruht auf einem biometrischen Merkmal (etwas, das das Subjekt ist, wie Iris, Netzhaut, Fingerabdruck),

- verhaltensbasierter Authentifizierungsfaktor: beruht auf Verhalten (etwas, das welches das Subjekt typischerweise macht, z.B. dynamisches Unterschriftsmuster).

Synonym: Authentifizierungsmerkmal

2.17 Authentifizierungsmittel

Ein Authentifizierungsmittel ist etwas, das ein Subjekt besitzt und das es unter seiner Kontrolle hat (typischerweise ein kryptographischer Schlüssel, ein Geheimnis oder ein biometrisches Merkmal). Ein Authentifizierungsmittel muss nicht unbedingt in Hardware Form vorliegen, sondern kann auch ein Soft-Token oder eine Software-Komponente sein. Ein Authentifizierungsmittel kann einen (single-factor authenticator) oder auch mehrere unabhängige Authentifizierungsfaktoren (multi-factor authenticator) benutzen (siehe auch Anforderungen an Authentifizierungsmittel).

Der vom Authentifizierungsmittel generierte Ausgabewert (engl. Authenticator output or authenticator response) wird durch eine mathematische Funktion (Authentifikator oder Authentifizierungsfunktion) aus einem geheimen Wert (z.B. privater Schlüssel), einem oder mehreren optionalen Aktivierungswerten (z.B. PIN oder biometrischer Informationen), und einem oder mehreren optionalen Eingabewerten (z.B. Zufallswerten oder Challenges) generiert. Im Trivialfall kann das Authentifizierungsmittel der geheime Wert selbst sein (z.B. im Fall eines

Passworts). Siehe Tabelle 3 für weitere Beispiele.

<!-- Todo: einfügen von Beispiele (ist im 170er) -->

Synonyme:

- Authenticator (siehe NIST 800-63-3 [3]), früher bei NIST 800-63-2 [4] als Token bezeichnet.
- Bei STORK als identity token bzw. authentication token bezeichnet

2.18 Authorization Provider

Entität, die Autorisierung als Dienstleistung anbietet.

2.19 Authorization Service

Der Service überprüft zur Ausführungszeit die Einhaltung der Rechte für die Nutzung der E-Ressource und erlaubt dem Subjekt die Nutzung, wenn es die entsprechenden Rechte besitzt.

2.20 Autorisierung

Administration: Definition der Zugangsregeln und Zugriffsrechte auf eine E-Ressource.

Zur Laufzeit: Prüfen von Zugriffsberechtigung eines authentifizierten Subjektes auf eine Ressource und erteilen des Zugriffs zur Laufzeit. Dabei wird zwischen Grob- und Feinautorisierung unterschieden.

2.21 Backend Attribute Exchange (BAE)

Attributabfrage im Hintergrund, üblicherweise durch eine Maschine. Ein Benutzer ist bei der Attributabfrage nicht direkt involviert, diese erfolgt ohne seine explizite Zustimmung.

2.22 Bearbeiten

Jeder Umgang mit Daten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten (kurz: Erstellen, Lesen, Verändern, Löschen, Übermitteln) von Daten.

2.23 Benutzerzentriertes Identitätsmanagement

Ermöglicht dem Benutzer die Auswahl spezifischer Credentials und Attribute zur Bearbeitung in Authentifikations- und Attribut-Anfragen und überlässt ihm so die Kontrolle über die eigene, digitale Identität. Das bedeutet nicht, dass der Benutzer jede Transaktion nochmals explizit genehmigen muss, aber dass die Daten immer durch die Identitätsverwaltung des Benutzers fliessen und direkt an seine digitale Identität gebunden sind.

2.24 Berechtigung

Recht eines Subjekts, bestimmte Ressourcen zu nutzen.

2.25 Bereich STIAM-Domäne

Als Bereich kann eine begrenzte Gruppe von Informationsbezügern und -lieferanten angesehen werden, welche ein bestimmtes Set an Attributen und eine gemeinsame Policy teilen. Die Semantik und Syntax dieser Attribute werden durch die Teilnehmer der Gruppe bestimmt. Beispielsweise soll es möglich sein, dass sich innerhalb von SuisseTrustIAM eine Teilföderation bilden kann, welche nur ihre intern bekannten Identitäten und Attribute über die Plattform austauscht.

2.26 Beweismittel

Ein Beweismittel für die Identitätsüberprüfung ist ein Dokument oder Objekt aus einer verlässlichen Quelle, das Angaben zum Antragsteller enthält.

Ein Beweismittel muss den Namen des Antragsstellers enthalten. Es kann einen eindeutigen Identifikator, körperliche und biometrische Merkmal aber auch beliebige andere Angaben des Antragstellers enthalten. Es sollte Sicherheitsmerkmale enthalten, die ein Reproduzieren erschweren.

Beispiele:

- Beglaubigte Urkunde
- Kreditkarten
- Fahrausweis
- Identitätsdokumente

2.27 Biometrisches Merkmal

Ein biometrisches Merkmal ist ein körperliches Merkmal eines Menschen, das es erlaubt diesen hinreichend von anderen zu unterscheiden, welches also zu dessen Identifizierung verwendet werden kann. Ein biometrisches Merkmal sollte sich im Laufe der Zeit wenig ändern. Kombinationen mehrere Merkmale sind dabei möglich, z.B. Erfassung des Gesichtes kombiniert mit Stimmerkennung.

Zu den wichtigsten biometrischen Merkmalen gehören:

- Fingerprint
- (dynamische) Unterschrift
- Gesichtsgeometrie
- Gesichtsbild (Foto)
- Irismuster
- Retina (Netzhaut)

- Handgeometrie
- Fingergeometrie
- Ohrform
- Stimme (Klangfarbe)
- DNA
- Geruch
- Tastenanschlag

Zur Identifizierung von natürlichen Personen werden zurzeit meist nur

- Fingerprint
- Iris
- Retina
- Gesichtsgeometrie
- Gesichtsbild (Foto)

Verwendet.

Biometrische Merkmale können bezüglich Funktion, Sicherheit, Fälschbarkeit und Anwendungsfreundlichkeit ebenfalls klassifiziert werden. Das NIST hat mit ihrer Online-Dokumentation „Strength of Function for Authenticators – Biometrics“ [ref] kurz SOFA-B dazu einen ersten Beitrag geleistet

2.28 Broker Service

Dieser Service vermittelt zwischen dem Subjekt, Ressourcen und den Services der Ausführungszeit, föderiert Authentifizierung und Attributwertbestätigung.

2.29 Certificate Authority/Certification authority (CA)

Eine Certificate Authority ist ein spezieller Credential Service Provider (CSP), der digitale Zertifikate (Public Key Zertifikate, e.g. X.509) als Authentifizierungsmittel ausgibt, erneuert und revoziert.

Synonyme: Certification Service Provider, Trust Service Provider (TSP)

Synonyme deutsch: Zertifizierungsstelle für digitale Zertifikate, Vertrauensdiensteanbieter

2.30 Community Metadaten

Signierter Zusammenzug von Entitätsmetadaten der Mitglieder einer STIAM-Community.

2.31 Client

Technische Einrichtung (Anwendung, Webbrowser etc.), mit der das Subjekt auf die Ressource zugreift.

2.32 Client Plattform

Die Client Plattform ist das System oder Gerät, von welchem das Subjekt einen Authentisierungsprozess anstösst. Dies kann beispielsweise ein Browser auf einem PC oder eine Applikation auf einem mobilen Gerät sein.

Synonym: user agent

2.33 Credential

Ein Credential stellt eine Menge von Daten (keine Hardware oder andere physische Container) dar, mit der eine elektronische Identität (E-Identity) an ein Authentifizierungsmittel gebunden wird, welches vom Subjekt besitzt und kontrolliert wird.

Das Credential ist ein Nachweis der behaupteten E-Identity. Je nach verwendeten Authentifizierungsfaktoren kann dies z.B. der Hash eines Passwortes, ein Abbild eines biometrischen Merkmals oder ein Zertifikat sein, das zur Definitionszeit von einem CSP an eine E-Identity gebunden wurde.

Ein Credential kann zur Authentifizierung, zur Identifizierung oder zur Autorisierung oder für eine Kombination dieser 3 Prozesse verwendet werden.

Ein Credential muss immer auf Authentizität und Vertrauenswürdigkeit überprüft werden, bevor es verwendet wird.

(siehe auch ISO 29115 [5], Annex B und NIST SP 800-63B [6], Kap 3).

Synonym: Identitätsnachweis

2.34 Credential Service

Der Credential Service gibt Authentifizierungsmittel aus und verwaltet sie. Er ermöglicht eine benutzerfreundliche Erneuerung bzw. den Ersatz von Authentifizierungsmitteln. Ein Authentifizierungsmittel bezieht sich auf eine E-Identity und ist auf ein bestimmtes Subjekt ausgestellt.

2.35 Credential Service Provider (CSP)

Ein Credential Service Provider ist eine Entität, die als vertrauenswürdiger Herausgeber von digitale Zertifikaten und anderer Sicherheits-Tokens (Authentifizierungsmitteln) agiert.

Der CSP kann eine eigene Registration Authorities (RA) enthalten und Dienste zur Verifizierung der Credentials (Identity Provider) umfassen. Ein CSP kann als öffentliche Instanz auftreten, oder als Dienst in eine abgeschlossene Domäne integriert sein.

2.36 Definitionszeit

In der Definitionszeit wird das IAM-System eingerichtet und konfiguriert. Die Definitionszeit umfasst damit die Prozesse zur Bereitstellung aller notwendigen Informationen für alle beteiligten Komponenten.

2.37 Digitales Zertifikat / Digital Certificate

Strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen (auch Zertifikat oder Public-Key-Zertifikat).

2.38 Ding

Ein Ding ist ein physischer Gegenstand, welcher über ein Netzwerk erreichbar ist. Innerhalb des Netzwerkes ist das Ding mit einem Identifikator identifizierbar. Mehrere Dinge, welche im selben Netzwerk verknüpft sind, bilden ein Internet der Dinge (Internet of Things IoT).

Synonyme: Objekt, Thing (IoT)

2.39 Discovery Service (WAYF - Where Are You From)

Der Discovery Service ist dafür zuständig, den Benutzer zu einem Identity Provider seiner Wahl zwecks Authentifizierung zu leiten.

2.40 Domäne

Administrative / technische Gemeinschaft oder Organisation mit einer gemeinsamen Policy.

2.41 E-Identity

Eine E-Identity ist die Repräsentation eines Subjekts. Eine E-Identity (digitale Identität) hat einen Identifikator (eindeutiger Name), meist zusammen mit einer Menge von zusätzlichen Attributen, welche innerhalb eines Namensraumes eindeutig einem Subjekt zugewiesen werden können. Ein Subjekt kann mehrere E-Identities haben.

Eine notifzierte E-Identity ist eine E-Identity, die alle in eIDAS 910/2014 [7] Artikel 7 aufgeführten Voraussetzungen erfüllt muss.

Synonyme: Digitale Identität, Digital Identity, Elektronische Identität, Electronic Identity

2.42 E-Identity Service

Der E-Identity Service stellt zu Subjekten E-Identities aus und verwaltet sie.

2.43 E-Ressource

Digitale Repräsentation einer Ressource. Eine E-Ressource hat einen Identifikator (eindeuti-

ger Name, oft URL/URI), welche innerhalb eines Namensraumes eindeutig einer Ressource zugewiesen werden kann. Eine Ressource kann mehrere E-Ressourcen haben.

2.44 E-Ressource Service

Der E-Ressource Service stellt zu Ressourcen E-Ressourcen aus und verwaltet sie.

2.45 Entität / Entity

Ein aktives Element eines IT Systems, z.B. ein automatisierter Prozess oder eine Menge von Prozessen, ein Teilsystem, eine Person oder eine Gruppe von Personen mit definierten Funktionalitäten. [SAMLGlossar]

Organisation mit definierter Rolle innerhalb einer STIAM-Community.

2.46 Elektronisches Identifizierungsmittel

Begriff aus eIDAS 910/2014 [7]: „Elektronisches Identifizierungsmittel“ ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird.

Ein elektronisches Identifizierungsmittel enthält Authentifizierungsfaktoren, Attribute für Personen und hat eine Gültigkeit. Bei einer (dynamischen) Authentifizierung wird der gesamte Prozess Subjekt authentifizieren vom elektronischen Identifizierungsmittel abgewickelt. Es umschliesst daher sowohl Authentifizierungsmittel, Credential und IdP. Das Ergebnis einer Authentifizierung mit einem elektronischen Identifizierungsmittel ist eine Authentifizierungsbestätigung, mit der die Identität des Subjekts und die erfolgreiche Authentifizierung bestätigt werden.

Beispiele für elektronische Identifizierungsmittel sind der neue deutsche Personalausweis (nPA) inkl. Middleware (AusweisApp) oder die gesamte SuisseID Infrastruktur bestehend aus SuisseID Token, Middleware (Gerätetreiber) und SuisseID IdP.

2.47 Elektronisches Identifizierungssystem

Begriff aus eIDAS 910/2014 [7]: *„Elektronisches Identifizierungssystem“ ist ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden.

Ein notifiziertes elektronisches Identifizierungssystem muss alle in eIDAS 910/2014 [7] Artikel 7 aufgeführten Voraussetzungen erfüllen.

2.48 Elektronisches Identifizierungssystem

Begriff aus eIDAS 910/2014 [7]: *„Elektronisches Identifizierungssystem“ ist ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die juristische Personen vertreten, elektronische Identifizie-

rungsmittel ausgestellt werden.

Ein notifiziertes elektronisches Identifizierungssystem muss alle in eIDAS 910/2014 [7] Artikel 7 aufgeführten Voraussetzungen erfüllen.

2.49 Empfängerbaustein

Der Empfängerbaustein realisiert eine standardisierte STIAM-Schnittstelle für eine Relying Party, welche die STIAM-Protokolle nicht direkt unterstützt (vgl. Abbildung 2).

2.50 Entitätsmetadaten

Metadaten einer AA oder RP zur Definition der Rolle einer Entität innerhalb der STIAM-Community.

2.51 Feinautorisierung

Gewährung bzw. Verweigerung des Zugriffs auf einzelne von einer Ressource bereitgestellten Funktionen oder Daten.

2.52 Föderierung / Federation

Eine Identitäts-Föderierung ist eine Zusammenarbeit verschiedener Entitäten über Organisations- und Systemgrenzen hinweg, ohne Duplikation oder Replikation der dazu notwendigen Benutzerdaten (E-Identities).

Eine Föderierung von Identitäten erlaubt es Informationen über eine Authentifizierung eines Subjektes und optional Identitätsinformationen zu diesem Subjekt über ein Netzwerk zu übermitteln.

Wie in Abbildung [ref] dargestellt besteht ein föderiertes Identitätssystem aus den drei Entitäten Subjekt, Relying Party (RP) und einem Identity Provider (IdP). Je nach Ausprägung des verwendeten Protokolls ist die Abfolge der Informationen anders. Das Subjekt kommuniziert dabei aber immer mit dem IdP, wie auch mit der RP. Das Subjekt authentisiert sich gegenüber dem IdP in einem primären Authentisierungsverfahren mit einem bestimmten Authentifizierungsmittel (Authenticator). Dieses Ereignis wird dann in Form einer Authentifizierungsbestätigung an die vertrauende Partei über das Netzwerk weitergegeben. Der IdP kann dieser Authentifizierungsbestätigung noch weitere (Personen-)Attribute zum authentisierten Subjekt beifügen.

Todo: Abbildung 5 aus 170er

Synonyme: föderiertes Identitätssystem, föderiertes IAM-System

2.53 Funktion

Eigenschaft, die einem Subjekt bestimmte Aufgaben, Kompetenzen und Verantwortung in-

nerhalb einer Organisation zuweist. Ein Subjekt kann mehrere Funktionen haben (vgl. Rolle).

2.54 Grobautorisierung

Gewährung bzw. Verweigerung des Zugangs zu einer Ressource.

2.55 Globally Unique Identifier GUID

Eindeutige Nummerierung, einem Subjekt zugeordnet, generiert bei dessen Registrierung auf der STIAM-Plattform. Verbindet die Einträge eines Subjekts in STIAM-UIR und STIAM-UCR.

2.56 GUID

Eine GUID ist die auf dem STIAM-Hub abgelegte, eindeutige Identität eines Subjekts, an welche die LinkedID in dessen Link Table geknüpft werden.

2.57 IAM-Dienstanbieter

Der IAM-Dienstanbieter ist Betreiber von einem oder mehreren IAM-Geschäftsservices gemäss Kapitel todo!.

2.58 Identifikator

Eine Zeichenkette, welche ein E-Identity oder eine E-Ressource innerhalb eines Namensraumes eindeutig bezeichnet. Der Identifikator einer Ressource ist oft eine URL/URI.

2.59 Identifizierung

Identifizierung ist ein Vorgang zur Definitionszeit, bei welchem die Identität des Subjekts meist mit Hilfe von Beweismitteln überprüft wird. Die Identifizierung wird meist durch eine Registration Authority (RA) durchgeführt.

Synonym: Identitätsfeststellung

2.60 Identität / Identity

Identität ist die Gesamtheit der ein Subjekt kennzeichnenden und als Individuum von allen anderen unterscheidenden Eigentümlichkeiten. Im IAM-Kontext wird hauptsächlich die E-Identity eines Subjekts verwendet (siehe E-Identity).

2.61 Identitäts- und Zugriffsverwaltung / Identity und Access Management (IAM)

Alle Prozesse und Systeme um Subjekten den Zugriff auf die Ressourcen zu ermöglichen, die diese auf Grund ihrer Funktion in der Organisation benötigen.

2.62 Identitätsdokument

In der Schweiz gelten die folgenden Dokumente als Identitätsdokumente:

- Reisepass
- Schweizer Identitätskarte
- eine für die Einreise in die Schweiz anerkannte Identitätskarte

2.63 Identity Linking

Identity Linking ist der Vorgang, bei welchem eine LinkedID an eine eindeutige, digitale Identität eines Subjekts geknüpft wird. Die dazu notwendigen Informationen werden in einer Link Table abgelegt.

2.64 Identity Provider (IdP)

Entität, die E-Identity verwaltet und herausgibt. Ein IdP stellt einen Authentication Service und meist auch einen Attribute Assertion Service zur Verfügung.

2.65 Identity Provider/ Attribut-Autorität (IdP/AA)

Im SuisseTrustIAM-Kontext können Unternehmen und Organisationen als Informationslieferanten eine IdP/AA-Komponente bereitstellen, welche als IdP agiert, aber auch zu einer ihr bekannten Identität Informationen in Form von Attributen ausstellen kann. Die Anforderungen an einen solchen IdP/AA und dessen Funktionen werden in den SuisseTrustIAM Dokumenten genauer beschrieben (vgl. auch STIAM-IdP, STIAM-Sender und Abbildung 2 todo).

2.66 Juristische Person

Juristische Personen sind nach Art. 52 ff ZGB sowie gemäss den einschlägigen Bestimmungen des Gesellschaftsrechtes des OR.

Eine juristische Person ist eine spezielle Organisation, die auf einem Vertrag von zwei Organisationen (der juristischen Person und der anerkennenden Behörde) beruht.

Juristische Personen können nur durch natürliche Personen handeln und sind daher immer an eine natürliche Person gebunden.

2.67 Körperliches Merkmal

Ein körperliches Merkmal ist ein Merkmal eines Menschen, wie Körpergrösse und Augenfarbe. Spezielle körperliche Merkmale sind die biometrischen Merkmale (siehe [ref] Kap. 3.7 eCH-0170).

2.68 Laufzeit

Zur Laufzeit finden die elektronischen Prozesse statt, mit denen ein Subjekt – im Erfolgsfall - Zugang und Zugriff auf die Ressourcen einer Relying Party erhält.

Synonym: Ausführungszeit

2.69 LinkedID

Im organisationsübergreifenden Kontext erlaubt LinkedID, E-Identities aus verschiedenen Domänen miteinander in Beziehung zu setzen. E-Identities können mit LinkedIDs zu einem beliebigen gerichteten Graphen verkettet werden. Die konkrete Umsetzung von eCH-0107 kann die Form zusätzlich einschränken (z.B. statt Graph nur Baumstruktur) und regelt entsprechend ihrer Fähigkeiten die Interpretation (Semantik) des Graphen. (vgl. todo!).

2.70 Linking Protokoll

Der Benutzer kann IdPs oder AAs in der Link Table seines Accounts verbinden. Um den korrekten Identifikator als Eintrag in der Link Table zu erhalten, muss sich der Benutzer gegenüber dem jeweiligen Authentisierungsservice authentifizieren. Dadurch kann ein eindeutiger Identifikator zwischen STIAM-Hub und dem IdP oder der AA ausgetauscht werden.

2.71 Logging Service

Der Service dokumentiert zur Ausführungszeit die Verwendung eines Services und stellt der Support-Organisation die notwendigen Informationen bereit, um Nutzungsprobleme oder Fehler aufzuklären.

2.72 Meta-Attribut

Bestandteil des Attribut-Schemas, Spezifizierung des Attributs.

2.73 Metadaten

Ein Mittel, um Vertrauen und technische Interoperabilität zwischen SAML Komponenten (Entitäten) zu ermöglichen. Können auch verwendet werden, um Attributinformationen auszutauschen.

2.74 Metadaten (Metadata)

In SuisseTrustIAM werden die Metadaten innerhalb des Organisations- und Komponenten-managements für die jeweils registrierten STIAM-Komponenten zentral in der STIAM-Hub Datenbasis abgelegt. Die Metadaten beschreiben die Komponenten der registrierten Organisationen und Provider mit ihren Federation-Service-Endpunkten, Zertifikaten und den angeforderten bzw. zur Verfügung gestellten Attributen.

2.75 Meta-Domäne

Domäne, welche die Zusammenarbeit zwischen zwei oder mehreren Domänen regelt.

2.76 Namensraum

Anwendungsbereich (z.B. ein Unternehmen, ein Staat, eine Fachgemeinschaft, eine Sprachgemeinschaft), für welchen die Bedeutung einer Zeichenkette (z.B. Identifikator) definiert ist.

2.77 Natürliche Person

Natürlich Person gemäss OR.

Synonyme: Benutzer, User

2.78 Netzwerk

Informationssystem welches in der Lage ist, Informationen mit verschiedenen verbundenen Komponenten auszutauschen.

2.79 OpenID Connect

OpenID Connect 1.0 (OIDC) [2] definiert eine einfache Identitätsschicht auf der Basis von OAuth 2.0 (RFC 6749), die auch von Mobilgeräten verwendet werden kann. OIDC verwendet das Basisprotokoll OAuth sowohl für die Authentisierung als auch für die Zugangskontrolle. Als Security-Tokens werden JSON Web Tokens [ref] verwendet.

2.80 Organisation

Eine Organisation ist eine organisatorische Einheit aus mehreren natürlichen Personen. Eine Organisation kann (Unter-)Organisationen enthalten.

2.81 Policy

Schriftlich festgehaltene Regelungen und Vorschriften, welche einzuhalten sind.

2.82 Quality Authentication Assurance (QAA)

Qualität der Authentifikation einer digitalen Identität gemäss ISO 29115:2013.

2.83 Register

Verzeichnisse in der Verwaltungssprache, wie z.B. die Einwohnerregister, Anwaltsregister, Zivilstandsregister, Handelsregister etc. Sie werden in der Regel von offiziellen Stellen (Behörden) geführt.

2.84 Registrierung / Registration

Prozess einer Registrierungsstelle, bei dem ein Subjekt eine E-Identity mit dazugehörigem Credential erlangt.

2.85 Registrierungsstelle/Registration Authority (RA)

Eine Registrierungsstelle ist eine Entität, die genügend Informationen zu einem Subjekt erfasst und überprüft, um dessen Identität überprüfen zu können.

Die RA kann ein integraler Bestandteil eines CSP sein oder als eigener Dienst im Auftrag des CSP handeln.

2.86 Relying Party (RP)

Die Relying Party vertritt die Interessen der Ressource. Sie nutzt IAM-Geschäftsservices und verarbeitet Informationen von IAM-Dienstanbietern für den Schutz seiner Ressourcen. Sie braucht zur Beurteilung der Berechtigung eines Ressourcenzugriffs nähere Informationen zu einem Subjekt.

Synonyme: Informationsbezüger, Informationskonsument, Lösungsanbiete

2.87 Ressource

Service oder Daten, auf welche ein Subjekt zugreifen kann, wenn es sich authentisiert hat und es auf der Basis der benötigten Attribute autorisiert wurde. Dies schliesst physische Ressourcen wie Gebäude und Anlagen, deren Benutzung über IT-Systeme gesteuert wird, ein.

2.88 Ressourcen-Verantwortlicher

Verantwortliche Stelle für die von der Relying Party verwalteten Ressourcen (z.B.: Anwendungsverantwortlicher, Serviceverantwortlicher, Dateninhaber).

2.89 Role based Access Control (RBAC)

Verfahren zur Zugriffssteuerung und -kontrolle auf Dateien oder Dienste (Deutsch: Rollenbasierte Zugriffskontrolle).

Bei der rollenbasierten Zugriffskontrolle werden Benutzern oder Gruppen von Benutzern eine oder mehrere Rollen zugeordnet. Eine Rolle enthält eine Menge von Berechtigungen (Permissions), die die erlaubten Operationen auf einer Ressource beschreiben.vgl. ABAC

2.90 Rolle / Role

a) Organisation, Subjekt: Bestimmte Anzahl von Funktionen, die in einer Organisation ausgeführt werden. Einem Subjekt können eine oder mehrere Rollen zugeteilt werden.

b) E-Identity: Attribute, die die Rolle/Funktionen des Subjekts repräsentieren

c) System, Entität: Aufgabe und Zweck einer Entität in einer Föderation. Einer Entität können eine oder mehrere Rollen zugeteilt werden.

2.91 SAML 2.0

SAML (Security Assertion Markup Language) erlaubt es, Informationen über Authentifizierungs- und Attributinformationen zwecks Autorisierung standardisiert zwischen mehreren Teilnehmern auszutauschen. Der SAML-Standard [ref] beschreibt die Syntax und Regeln zum Anfordern, Erstellen und Austauschen von SAML-Assertions.

2.92 SAML 2.0 Web Browser SSO Profile

Profile fassen spezielle Anwendungsfälle von SAML zusammen. Das SAML 2.0 Web Browser SSO (single-sign-on) Profil [ref] beschreibt webbasierte Authentisierungsszenarien, inkl. Identity Federation, für Browser.

2.93 SAML Protokoll

OASIS hat mit der Einführung von SAML nicht nur das SAML Token, sondern auch ein Protokoll und Bindings definiert, welche die Übertragung der Token spezifizieren. SAML unterstützt unter anderem HTTP-POST und HTTP-Redirect als Request-Response Schema. Nebst SAML gibt es auch andere Protokolle, welche SAML Token unterstützen. Zwei Beispiele dafür sind WS-Federation und WS-Trust.

2.94 SAML Token

Ein SAML Token enthält bestätigte Identitätsinformationen eines Subjekts in standardisierter Form. Kernpunkt eines SAML Tokens ist die Assertion. Diese beschreibt, zu wem das Token gehört, wie lange es gültig ist, wer es ausgestellt hat und dann die Identitätsinformationen des Subjekts und allfällige Attribute, welche an dieses geknüpft sind.

2.95 Security Assertion Markup Language (SAML)

SAML (Security Assertion Markup Language) wurde spezifiziert, um herstellerunabhängig Single Sign-On zu ermöglichen. SAML ist ein XML Framework, mit dessen Hilfe Authentifizierungs- und Autorisierungsinformationen ausgetauscht werden können. SAML wurde von einem internationalen Konsortium und im Rahmen der OASIS standardisiert. [1]

2.96 Security Token

Ein Datenpaket, welches verwendet werden kann, um den Zugriff auf eine Ressource zu autorisieren.

Ein Security Token enthält bestätigte Identitätsinformationen eines Subjekts in standardisierter Form (Authentication Statement, Authentication Assertion). Eine Relying Party verifiziert und validiert diese Informationen, um daraus einen Zugangsentscheid abzuleiten.

2.97 Security Token Service STS

Infrastruktur, die in der Lage ist, Security Tokens nach SAML 2.0 Standard zu erzeugen, zu signieren und als Service zur Verfügung zu stellen.

2.98 Service Level Agreement (SLA)

Bezeichnet einen Vertrag zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen.

2.99 Senderbaustein

Der Sender-Baustein realisiert eine standardisierte STIAM-Schnittstelle zur Anbindung einer Attribut-Autorität, welche die STIAM-Protokolle nicht direkt unterstützt, an den STIAM-Hub (vgl. Abbildung 2).

2.100 STIAM

SuisseTrust Identity and Access Management

2.101 STIAM Certificate Authority (STIAM-CA)

Ein STIAM-CA ist ein CA, der von der STIAM-Community akzeptiert wird.

2.102 STIAM Identity und Attribute Bus

Vermittelt Authentisierungs- und Attributanfragen zwischen Subjekt, RP, AuthnA und AA.

Nimmt die SAML-Requests der STIAM-Empfänger entgegen und leitet sie an die korrekte AuthnA und AA weiter. Danach nimmt er die Responses der STIAM-Sender entgegen und

sendet die Informationen als aggregierte SAML-Response an die korrekte RP zurück.

2.103 STIAM-Account

Minimal gebildet durch Einträge in STIAM-IdP (E-Mail Addresse, Passwort, optionales 2. Kanal Authentifikationsmittel) und STIAM-UCR (GUID, STIAM-IdP-Identifikator, optionales Credential).

Wird bei der Registrierung des Subjekts erstellt, muss danach vom Subjekt aktiviert werden. Jedes Subjekt hat auf der STIAM-Plattform mindestens einen STIAM-Account.

2.104 STIAM-Broker

Die zentrale Vermittlerinfrastruktur zwischen Subjekt, RP, AuthnA und AA. Er besteht aus dem Identity und Attribute Bus, STIAM-RLM, STIAM-MDR, STIAM-IdP, STIAM-UIR und STIAM-UCR. Ist ein Broker gemäss eCH-0107.

Synonym: Vermittlerinfrastruktur

2.105 STIAM-Community

Die STIAM-Community bilden alle Teilnehmer, die mit einer STIAM-Plattform interagieren und die einheitliche Spezifikation (vgl. Policy) berücksichtigen.

2.106 STIAM-Empfänger

Kommunikationsmodul, das die standardisierte SAML-Kommunikation zwischen der RP und dem STIAM-Broker realisiert.

Der STIAM-Empfänger nutzt die Dienste des STIAM-Hubs, um einen Benutzer authentifizieren zu lassen und weitere Informationen über diesen zu beziehen, die dann zur Zugangssteuerung verwendet werden können. Der STIAM-Empfänger definiert, wie der Benutzer authentifiziert werden soll und welche Attribute in welcher Qualität notwendig sind, um Zugang auf eine seiner geschützten Ressourcen zu erlauben. Der STIAM-Empfänger erhält vom STIAM-Hub die geforderten Informationen in Form eines Security Tokens. Der STIAM-Empfänger ist eine Relying Party, beispielsweise ein Portal."

STIAM-Hub (Vermittler, Intermediär)

"Der STIAM-Hub als Kernstück der SuisseTrustIAM-Plattform hat zwei Funktionen. Erstens bietet er zur Definitionszeit die Trust- und E-Identity-Geschäftsservices an, indem sich Benutzer und Organisationen auf dem STIAM-Hub registrieren können und zweitens agiert er als Vermittler (Broker) zwischen den Entitäten zur Laufzeit. Die administrativen Aufgaben auf dem STIAM-Hub können grob in folgende Prozesse und Funktionen aufgeteilt werden (vgl. dazu die administrativen Prozesse in Kapitel 7):

User Management: Benutzer können auf dem STIAM-Hub einen User-Account eröffnen und diesen verwalten. Alternativ ist es auch möglich, dass ein System Administrator einer Organisation User-Accounts für einen (oder mehrere) Benutzer bzw. Maschinen erstellen kann.

Organisation Management: Eine Organisation wird vom SuisseTrustIAM Betreiber initial in der Datenbasis eröffnet. Ein Mitarbeitender der Organisation (in der Rolle eines Organisati-

onsverantwortlichen) wird dabei ermächtigt, bestimmte Eigenschaften der Organisation zu administrieren und zusätzliche Systemadministratoren zu erstellen und zu ermächtigen. Damit können administrative Aufgaben der Organisation aufgetrennt und delegiert werden (vgl. dazu die Definition der Rollen und Prozesse in der eCH-0169 SuisseTrustIAM-Geschäftsarchitektur [todo!]).

Komponenten Management: Ziel der zentralen Administration auf dem STIAM-Hub ist die einfache und selbstständige Verwaltung der STIAM-Komponenten durch deren Systemverantwortlichen. Dieser kann selbstständig einzelne Komponenten zu SuisseTrustIAM hinzufügen bzw. verwalten. Für diese Komponenten müssen bestimmte Parameter, welche für ihre Rolle innerhalb der STIAM-Plattform notwendig sind, erfasst und konfiguriert werden.

Attribut Management: Der SuisseTrustIAM Betreiber unterhält eine Liste von Attributen, welche in der SuisseTrustIAM-Community verwendet werden können.

2.107 STIAM-IdP

Interner IdP einer STIAM-Plattform. Dient dem Registrieren und Initialisieren von STIAM Accounts und liefert qualitativ minimale Authentifikation der Subjekte.

Ein Identity Provider hat in STIAM die Funktion, ein Subjekt zu authentifizieren. Ein STIAM-IdP implementiert eine standardisierte STIAM-Schnittstelle zum STIAM-Hub (vgl. Abbildung 2 [todo!]).

2.108 STIAM-Komponente

"Zu den STIAM-Komponenten gehören STIAM-Sender (Attribut-Autorität), STIAM-Empfänger (Relying Party), STIAM-IdPs, der STIAM-Hub und STIAM-CSPs. Die STIAM-Komponenten besitzen eine standardisierte Schnittstelle, die es ihnen erlaubt, miteinander zu kommunizieren und sich gegenseitig zu vertrauen.

Abbildung 2: STIAM-Komponenten"

2.109 STIAM-Metadata Repository (STIAM-MDR)

Zentraler Auskunftsdienst der STIAM-Plattform, verwaltet und publiziert die Metadaten für die STIAM-Community.

2.110 STIAM-Plattform

Die STIAM-Plattform umfasst den STIAM-Broker sowie alle zusätzlichen STIAM-spezifischen Komponenten (STIAM-Sender, STIAM-Empfänger, STIAM-CSP) die den Betrieb der funktionalen Lösung ermöglichen.

2.111 STIAM-RLM (Reporting-Logging-Monitoring)

Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden Zugriffe auf Ressourcen gespeichert. Mit dem STIAM-RLM sollen analog dazu alle Vorgänge, die vom STIAM-Broker vermittelt werden, geloggt und überwacht werden können.

2.112 STIAM-Sender

Kommunikationsmodul, das die standardisierte SAML-Kommunikation zwischen der AA und dem STIAM-Broker realisiert.

Der STIAM-Sender ist eine Attribut-Autorität (in der Regel Verzeichnisse oder Register), die Attribute für die STIAM-Community in standardisierter Form bereitstellt. Der STIAM-Sender hat ein standardisiertes Interface zum STIAM-Hub (vgl. Abbildung 2 aus 168 todo).

2.113 STIAM-UCR (User Credential Repository)

Enthält die Credentials der Subjekte und deren Quelle.

2.114 STIAM-UDR (Userdata Repository)

Der Datensafe eines Subjekts, in dem alle subjekt-spezifischen Attribute verwaltet werden, die nicht von einer externen AA bereitgestellt werden. Das Subjekt trägt seine Attribute hier selber ein. Die STIAM-UDR ist eine spezielle Ausprägung einer AA. Sie ist logisch von der STIAM-Plattform getrennt und kommuniziert mit dieser über einen STIAM-Sender.

2.115 STIAM-UIR (User Identifier Repository)

Die User Identifier Repository verwalten die externen Identifier-Definitionen zu AA-Ressourcen und ermöglicht es der STIAM-Plattform, so Daten über ein Subjektaus einer AA und die intern identifizierte Person zu matchen.

2.116 Subjekt

Ein Subjekt ist eine natürliche Person, eine Organisation (juristische Person), ein Service oder ein Ding, das auf eine Ressource zugreift oder zugreifen möchte. Ein Subjekt wird durch E-Identities repräsentiert.

Abbildung 6 Definition Subjekt ech-0170 → Todo: Bild einfügen

Ein Abonnent (engl. Subscriber, siehe NIST 800-63-3A [8]) ist ein Subjekt, welches nach erfolgreich abgeschlossenem Registrationsprozess (Prozess Subjekt registrieren) ein Authentifizierungsmittel von einer CSP erhalten hat. Damit wird das Subjekt zu einem autorisierten Teilnehmer in der Identity Federation Community.

Ein Antragsteller (engl. Applicant, siehe NIST 800-63-3A [8]), ist ein Subjekt, das in die Identity Federation Community aufgenommen werden möchte und dazu den Prozess Subjekt registrieren durchläuft. Wurde dieser erfolgreich abgeschlossen, wird aus dem Antragsteller ein Abonnent.

Ein Antragsteller (engl. Applicant, siehe NIST 800-63-3A [8]), ist ein Subjekt, das in die Identity Federation Community aufgenommen werden möchte und dazu den Prozess Subjekt registrieren durchläuft. Wurde dieser erfolgreich abgeschlossen, wird aus dem Antragsteller ein Abonnent.

Ein Überbringer (engl. Bearer) ist ein Subjekt, das eine vom IdP ausgestellte Authentifizierungsbestätigung an die RP übergibt."

2.117 Trust Service

Der Trust Service pflegt die akzeptierten, vertrauenswürdigen IAM-Dienstanbieter.

2.118 Trust-Level

Zwischen den Beteiligten abgemachtes Vertrauensniveau, das Sicherheitsanforderungen für die Prozesse und die technologischen Komponenten festlegt.

2.119 Trusted Third Party

Vertrauenswürdige Instanz, z.B. zur Verwaltung von öffentlichen Schlüsseln oder Zertifikaten.

2.120 UID-Einheit

Bei UID-Einheiten handelt es sich um alle Unternehmen und Institutionen, die eine UID erhalten. Im UID-System ist der Unternehmensbegriff weit gefasst. Unter UID-Einheit versteht man somit nicht nur alle in der Schweiz tätigen Unternehmen im eigentlichen Sinn, sondern alle «Kundinnen und Kunden der öffentlichen Verwaltung», die Charakteristiken eines Unternehmens aufweisen oder die zu rechtlichen, administrativen oder statistischen Zwecken identifiziert werden.

-> Siehe auch:
https://www.bfs.admin.ch/bfs/de/home/register/unternehmensregister/unternehmens-identifikationsnummer/uid-einheiten-unternehmen.html

2.121 Vermittler

Ein Vermittler bietet gemeinsame Dienste, wie Metadaten, Discovery oder Identity Linking, für alle anderen Stakeholder in einer Identity Föderation an. Siehe auch Broker Service, STIAM-Broker

2.122 Vertrauen

Formell meist im SLA definierte Vertrauensbeziehung zwischen verantwortlichen Stellen. z.B. die formelle Beschreibung der Kriterien, die erfüllt sein müssen, damit sich zwei Organisationen, Entitäten, Domänen etc. gegenseitig vertrauen (engl. Trust).

2.123 Verzeichnis

Systematische Sammlung von Informationen mit gemeinsamen Merkmalen.

2.124 WS-Federation

WS-Federation in der aktuellen Version 1.2 [ref → sind im 168 beschrieben] ist ebenfalls Teil

der WS-* Spezifikation und erweitert WS-Trust mit der Möglichkeit, Security Tokens auch über unterschiedliche Domains auszutauschen, indem der Standard mehrere Identity Provider unterstützt. Sowohl bei WS-Trust wie auch bei WS-Federation kann das SAML-Tokenformat als Security Tokens verwendet werden.

2.125 WS-Trust

Der von OASIS spezifizierte Web Service Trust (WS-Trust) [ref] in der aktuellen Version 1.4 ist Teil der WS-* Spezifikation, welche ein Framework für den sicheren Austausch von Web Service Nachrichten bereitstellt. Bei WS-Trust handelt es sich um einen Standard, der die Interoperabilität von Sicherheits-Token durch Definition eines Protokolls für Anforderungen und Antworten unterstützt. Dieses Protokoll ermöglicht einem Consumer (z.B. ein Web-Service-Client), den Austausch eines bestimmten Sicherheitstokens von einem anerkannten Aussteller, dem Security Token Service (STS), anzufordern und einer Relying Party zu übergeben.

2.126 Zugang Service

Der Service überprüft die Einhaltung der Zugangsregeln und erlaubt dem Subjekt den Zugang, wenn die entsprechenden Regeln erfüllt sind.

Synonym: Access Service

2.127 Zugangsregel

Ressourcenverantwortliche definieren die Zugangsregeln für ihre E-Ressourcen. Die Zugangsregeln definieren die Bedingungen, unter denen ein Subjekt Zugang zu einer Ressource erhält (Grobautorisierung), z.B. nach erfolgreicher Authentifizierung und Bestätigung bestimmter Attribute.

2.128 Zugangsregel Service

Der Service verwaltet die Regeln für den Zugang zu einer Ressource. Die Regeln sind auf der Basis von Authentisierung oder Attributen definiert.

2.129 Zugriff

Interaktion mit einer Entität um eine oder mehrere ihrer Ressourcen zu manipulieren und oder zu nutzen. [SAMLGlossar]

Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden Zugriffe gespeichert.

2.130 Zugriffskontrolle

Überwachung und Steuerung des Zugriffs auf Ressourcen. Das Ziel ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen.

2.131 Zugriffsrecht

Ressourcenverantwortliche definieren die Zugriffsrechte für ihre E-Ressourcen. Die Zugriffsrechte definieren die Bedingungen unter denen ein Subjekt auf die verschiedenen Funktionalitäten einer Ressource nutzen darf (Feinautorisierung), z.B. nach erfolgreicher Authentifizierung und Bestätigung bestimmter Attribute.

2.132 Zugriffsrecht Service

Der Service verwaltet die Rechte für die Nutzung einer E-Ressource. Die Rechte sind auf der Basis von Authentisierung, Attributen oder eigenen Modellen (Gruppen, Rollen, Einzelberechtigungen) definiert.

3 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellen oder welche **eCH** referenzieren, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

4 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen

Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen & Bibliographie

[1] N. Ragouzis, J. Hughes, R. Philpott, E. Maler, P. Madsen, and T. Scavo, “Security Assertion Markup Language (SAML) V2.0 Technical Overview (OASIS),” *May*, no. February, p. 50, 2007.

[2] Natsakimura, “OpenID Connect | OpenID.” [Online]. Available: http://openid.net/connect/. [Accessed: 10-Oct-2016].

[3] J. L. F. Paul A. Grassi, “DRAFT NIST Special Publication 800-63-3,” 2016. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html. [Accessed: 01-Sep-2016].

[4] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, W. E. Burr, D. F. Dodson, and R. A. Perlner, “NIST Special Publication 800-63-2 Electronic Authentication Guideline.”

[5] P. Editors, W. Fumy, M. De Soete, E. J. Humphreys, K. Naemura, and K. Rannenberg, “ITU-T Recommendation X . 1254 | International Standard ISO / IEC DIS 29115 Information technology — Security techniques — Entity authentication assurance framework,” 2011.

[6] J. P. R. Paul A. Grassi, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, James L. Fenton, “DRAFT NIST Special Publication 800-63B,” 2016. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html. [Accessed: 22-Aug-2016].

[7] D. A. S. Europ, I. Parlamentder, R. A. T. D. E. R. Europ, and I. Union, “VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom,” vol. 2014, no. 910, 2015.

[8] J. L. F. Paul A. Grassi, Jamie M. Danker, William E. Burr, “DRAFT NIST Special Publication 800-63A,” 2016. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63a.html. [Accessed: 01-Sep-2016].

Anhang B – Mitarbeit & Überprüfung

<Hier sind alle Mitarbeiterinnen und Mitarbeiter aufzuführen, die an dieser Version des Dokuments mitgearbeitet haben.>

<N. N.>	<Organisation/Firma>
<N. N.>	<Organisation/Firma>

Anhang C – Abkürzungen und Glossar

<Abk.>	<Text>
<Abk.>	<Text>

Anhang E – Abbildungsverzeichnis

Anhang F – Tabellenverzeichnis